

Claims

1. A method of controlling a network entity (4, 5) of a  
5 mobile communication network and a mobile station (1),  
wherein said network entity (4, 5) and said mobile  
station (1) are arranged to conduct a plurality of  
predetermined message exchange procedures in the course  
of which predetermined messages are exchanged between  
10 said network entity (4, 5) and said mobile station (1)  
depending on the given procedure, where said  
predetermined messages may be encrypted, an encrypted  
message being any message of which at least a part is  
encrypted, and where said network entity (4, 5) and said  
15 mobile station (1) are arranged to conduct one or more  
encryption key generation procedures during which the  
network entity (4, 5) and the mobile station (1)  
generate and store respective corresponding encryption  
keys, in order to be able to encrypt and decrypt  
20 exchanged messages, where said method comprises the  
steps of:
  - if said network entity (4, 5) receives a message from  
said mobile station (1), determining (S21) whether said  
received message is encrypted,
  - if the received message is encrypted, determining  
25 (S22) whether a correct encryption key for decrypting  
said message is available to said network entity (4, 5),  
and if no correct key is available, sending (S23) a  
predetermined triggering message to said mobile station  
30 (1),
  - upon receiving said predetermined triggering message,  
said mobile station (1) interrupting (S33) the procedure  
in the course of which it sent the encrypted message for  
which the network entity (4, 5) did not have a correct  
35 key, and initiating (S34) an encryption key generation  
procedure.

2. A method according to claim 1, wherein said messages are arranged such that they have a first part (61) and a second part (62), said first part (61) being an unencrypted part that is not allowed to be encrypted,  
5 and said second part (62) being encryptable.
3. A method according to claim 2, wherein said messages are arranged such that said first part (61) contains an encryption indication (611) of whether said second part  
10 (62) is encrypted or not; and said determining of whether the second part (62) of said received message is encrypted or not is achieved by analysing said encryption indication (611).
- 15 4. A method according to claim 2 or 3, wherein said messages are arranged such that said first part (61) contains a message type identifier (610) identifying the type of the message, and after having received a message from said mobile station (1), said network entity (4, 5)  
20 identifies the message type of said received message from the message type identifier (610) and determines whether said identified message type belongs to a predetermined category, and sends said predetermined triggering message to said mobile station (1) only if  
25 the message type of said received message falls into said predetermined category.
- 30 5. A method according to one of the preceding claims, wherein said one or more encryption key generation procedures comprise obtaining an encryption base value (RAND) commonly available to said network entity (4, 5) and said mobile station (1) at the time of conducting said encryption key generation procedure, and generating corresponding encryption keys in said network entity (4,  
35 5) and said mobile station (1) on the basis of said encryption base value (RAND).

6. A method according to claim 5, wherein said encryption base value (RAND) is a regularly changed value that is broadcast by said network to listening mobile station (1)s.

5

7. A method according to one of the preceding claims, wherein said encryption key generation procedure is conducted as a part of a registration procedure of said mobile station (1) with said network entity (4, 5).

10

8. A mobile station (1) arranged to operate with a mobile communication network, comprising

15

an encryption key generator (1321) for generating a encryption key,

an encryption key memory (131) for storing a generated encryption key,

20

a message encryptor/decryptor (1322) for encrypting messages sent to said mobile communication network and decrypting messages received from said mobile communication network using a stored encryption key, an encrypted message being any message of which at least a part is encrypted,

30

a controller (1323) for controlling the operation of said mobile station (1), said controller being arranged to perform one or more predetermined message exchange procedures with said mobile communication network, in the course of which said mobile station (1) sends predetermined types of messages to said mobile communication network and waits for predetermined corresponding types of messages from said mobile communication network, said controller furthermore being arranged to identify the receipt of a predetermined triggering message from said mobile communication

35

network during the course of an ongoing message exchange procedure, and in response to said predetermined triggering message interrupting the ongoing message exchange procedure and initiating an encryption key generation procedure.

5        9. A mobile station (1) according to claim 8, wherein said controller (1323) is arranged to conduct said encryption key generation procedure as a part of a registration procedure of said mobile station (1) with said mobile communication network.

10      10. A network entity (4, 5) of a mobile communication network arranged to communicate with a mobile station (1), comprising:

15      an encryption key generator (511) for generating a encryption key,

20      an encryption key memory (51) for storing a generated encryption key,

25      a message encryptor/decryptor (421) for encrypting messages sent to said mobile station (1) and decrypting messages received from said mobile station (1) using a stored encryption key, an encrypted message being any message of which at least a part is encrypted,

30      a controller (51) for controlling the communication between said network entity (4, 5) and said mobile station (1), said controller (51) being arranged to determine whether messages received from said mobile station (1) are encrypted or not, and if a received message is encrypted, determining whether a correct key for decrypting said message is available to said network entity (4, 5), and if no correct key is available, sending a predetermined triggering message to said

mobile station (1) for triggering an immediate encryption key generation procedure in said mobile station (1).